Failure Modes and Effects Analysis/Critical Items List For The Input Output Processor Package (IOP)

Fluids and Combustion Facility Combustion Integrated Rack

Preliminary
October 27, 2000

AUTHORIZED by CM when under FORMAL Configuration Control	
Date	Signature
10/27/00	*/s/ A. Germovsek*

Prepared For:
National Aeronautics and Space Administration
John H. Glenn Research Center
Microgravity Science Division
Cleveland, Ohio 44135

Prepared By:
Federal Data Corporation
Under Contract NAS3-99155
2001 Aerospace Parkway
Brook Park, Ohio 44142

PREFACE

The National Aeronautics and Space Administration (NASA) is developing a modular, multi-user experimentation facility for conducting fluid physics and combustion science experiments in the microgravity environment of the International Space Station (ISS). This facility, called the Fluids and Combustion Facility (FCF), consists of three test platforms: the Fluids Integrated Rack (FIR), the Combustion Integrated Rack (CIR), and the Shared Accommodations Rack (SAR). This document is intended to produce a Failure Modes and Effects Analysis/Critical Items List for the Input Output Processor (IOP) contained in the Combustion Integrated Rack (CIR).

FAILURE MODES AND EFFECTS ANALYSIS/CRITICAL ITEMS LIST FOR THE FLUIDS AND COMBUSTION FACILITY COMBUSTION INTEGRATED RACK IMAGE PROCESSING PACKAGE

Prepared By: _/s/ Thomas J. Young_ **Date:** _10/27/00_
Thomas J. Young
Reliability Engineer
Hernandez Engineering Inc.

Approved By: _/s/ Jon Wetherholt_ **Date:** _10/27/00_
Jon Wetherholt
Systems Lead
Analex Corporation

Approved By: _/s/ William Quinn_ **Date:** _10/26/00_
William Quinn
Product Assurance Manager
Hernandez Engineering Inc.

Concurred By: _/s/ Andrew M. Peddie_ **Date:** _10/27/00_
Andrew M. Peddie
FCF Deputy Director
Federal Data Corporation

Concurred By: _/s/ Christopher J. Pestak_ **Date:** _10/27/00_
Christopher J. Pestak
FCF Director
Analex Corporation

REVISION PAGE
FAILURE MODES AND EFFECTS ANALYSIS/CRITICAL ITEMS LIST

Revision	Date	Description of Change or ECO's/ECP's Incorporated	Verification and Date
Preliminary	10/27/00	Initial release for PDR	10/27/00

TABLE OF CONTENTS

LIST OF APPENDICES

LIST OF TABLES

LIST OF FIGURES

1.0 INTRODUCTION

1.1 Purpose.

This document presents a preliminary Failure Modes and Effects Analysis (FMEA) and a Critical Items List (CIL) for the Input Output Processor (IOP) of the Combustion Integrated Rack (CIR), which is part of the Fluids and Combustion Facility (FCF) that will be deployed on the International Space Station (ISS). This preliminary FMEA/CIL is intended to determine the possible functional failure modes and their effects on the IOP and subsequently the CIR, the FCF, and the ISS. This analysis shall promote design improvements, and to promote early considerations of corrective actions in response to various failures. The CIL points to certain items/functions that thru specified failure modes could result in critical safety hazards or loss of capability to adequately perform the science experiments associated with the CIR.

1.2 Scope.

This preliminary analysis is restricted to the IOP of the CIR and is not intended as an analysis of other CIR subsystems, FCF systems or space station vehicle hardware of any type. This FMEA/CIL is not intended to analyze the detailed "structure" or composition of

1. FCF software code
2. Software fault tolerance
3. Software design to initiate commands and control
4. Human error
5. Support structure and tubing
6. Electrical wiring
7. Electronic enclosures
8. Mechanical linkages such as power bolts, gears, and cranks.

1.3 Order of precedence for verification requirements

The verification requirements contained in this document shall take precedence over any conflicting verification requirements.

2.0 DOCUMENTS

This section lists specifications, models, standards, guidelines, handbooks, and other special publications. These documents have been grouped into two categories: applicable documents and reference documents.

Applicable Documents	
SSP 30234	Failure Modes and Effects Analysis and Critical Items List Requirements for Space Station

Reference Documents	
SSP 50431	Space Station Program Requirements for Payloads
SARGE	Standard Assurance Requirements and Guidelines for Experiments
CIR-PLAN-A-003	CIR Flight Safety Data Package
CIR-SDP-000	CIR Delta Phase 1 Safety Data Package
FCF-DOC-003	Combustion Integrated Rack Baseline System Description

2.1 Order of precedence for documents

In the event of a conflict between this document and other documents referenced herein, the requirements of this document shall apply. In the event of a conflict between this document and the contract, the contractual requirements shall take precedence over this document. All documents used, applicable or referenced, are to be the issues defined in the Configuration Management (CM) contract baseline. All document changes, issued after baseline establishment, shall be reviewed for impact on scope of work. If a change to an applicable document is determined to be effective, and contractually approved for implementation, the revision status will be updated in the CM contract baseline. The contract revision status of all applicable documents is available by accessing the CM database. Nothing in this document supersedes applicable laws and regulations unless a specific exemption has been obtained.

2.2 Applicable documents

The documents in these paragraphs are applicable to the FCF Project to the extent specified herein.

2.3 Reference Documents

The documents in this paragraph are provided only as reference material for background information and are not imposed as requirements.

2.4 General Approach

After having established a mutual understanding of the functionality of the various major components of the system, CIR designers and reliability engineering have worked together to determine failure modes. Failure modes associated to a particular component/system have been described along with the component function, failure mode criticality, local failure effect, system effect, station/crew effect, potential failure mode cause, failure detection method, and compensating provisions. For PDR, the current concept for failure detection and compensating provisions was noted but is subject to change as our understanding of design and operations improves.

3.0 OVERVIEW OF CIR INPUT / OUTPUT PACKAGE

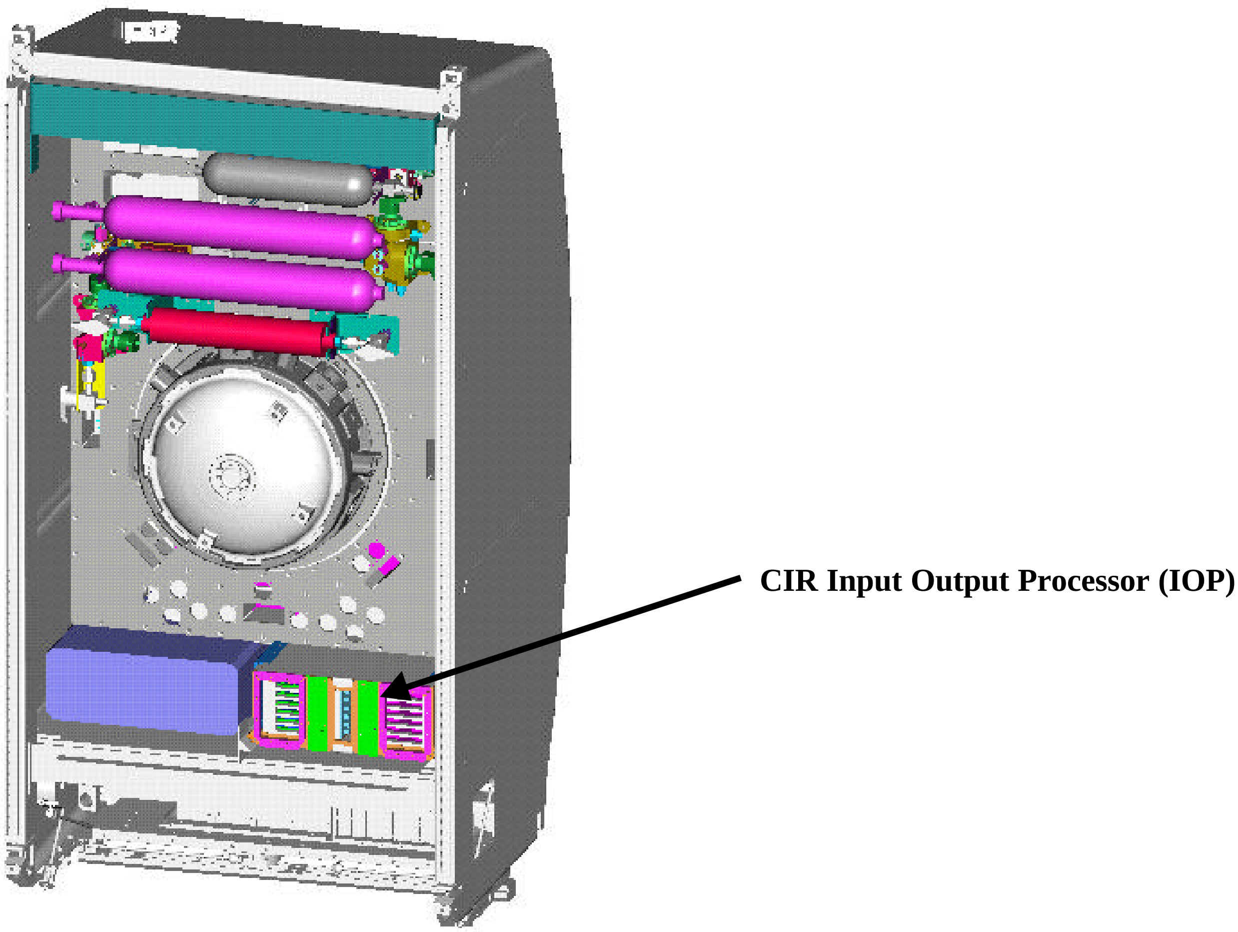
3.1 System Description

The CIR IOP performs the command processing, data processing, data management, caution and warning, health and status monitoring, and time synchronization for the facility.

The IOP incorporates the following features:

- 14-slot, 6U VME64x Bus Architecture, divided into 2 backplanes, 7-slots each
- 2 – 73.4 Gigabyte Wide SCSI fast hard disk drives for data buffering
- Power Supplies and EMI Filtering

The IOP is the primary controller for the CIR. The IOP commands the EPCU to power on and off the loads individually or in any combination. The IOP also is the command and data interface with the station for the CIR. This activity includes commands from the ground and laptop to perform experiments, functions to render the system safe, and downlink data.



3.2 Interface Connections

The IOP provides the data and command paths to/from the Space Station and between other subsystems within the Combustion Integrated Rack (CIR).

- MIL-STD-1553B –LRDL interface and ECS/ARIS control
- Ethernet Switch – MRDL interface
- Fiber Optic Interfaces for three rack FCF LAN
- High Rate Data Link (HRDL) to Interface
- Analog video routing – Video switch and CVIT
- Fiber Optic Converter for rack to rack analog video

- Power Distribution and communications with SAM-FF
- CANbus – dual independent channel for Optics Bench and ECS C&C and H&S data collection.
- Fiber Optic Converter for rack to rack diagnostic communications
- Removable hard drives for storage of science data
- Sync Generator
- Fiber Optic Converters for rack to rack Sync Bus
- Laptop Interface
- Two 28Vdc @ 4Adc circuits, provided to the IOP from the EPCU
  (These circuits are paralleled inside the IOP)
- One 28Vdc @4Adc (112 W) circuit routed through the IOP for SSC power.
- +/- 15Vdc routed to SAMS-FF TSH

3.2.1 Downlinking Interfaces

All data to be downlinked to the ISS must come through the CIR IOP via Ethernet, 1553B or analog interfaces. The CIR IOP receives science, and ancillary data via the Ethernet. The data is then formatted and downlinked via the 1553B, HRDL or MRDL interfaces.

3.2.2 Analog Input/Output and Communication Channels

Analog inputs are used for interfacing with pressure transducers, thermistors, current sensors, power monitoring, flow meters, and any additional instrumentation required for science, health and status monitoring for all packages within the rack.

Analog outputs for commanding set points of system effectors to control parameters such as flow rates, fan speed, energy levels, etc.

For general-purpose command and control applications, data transfer, etc. - MIL-STD-1553B, 10BaseT Ethernet

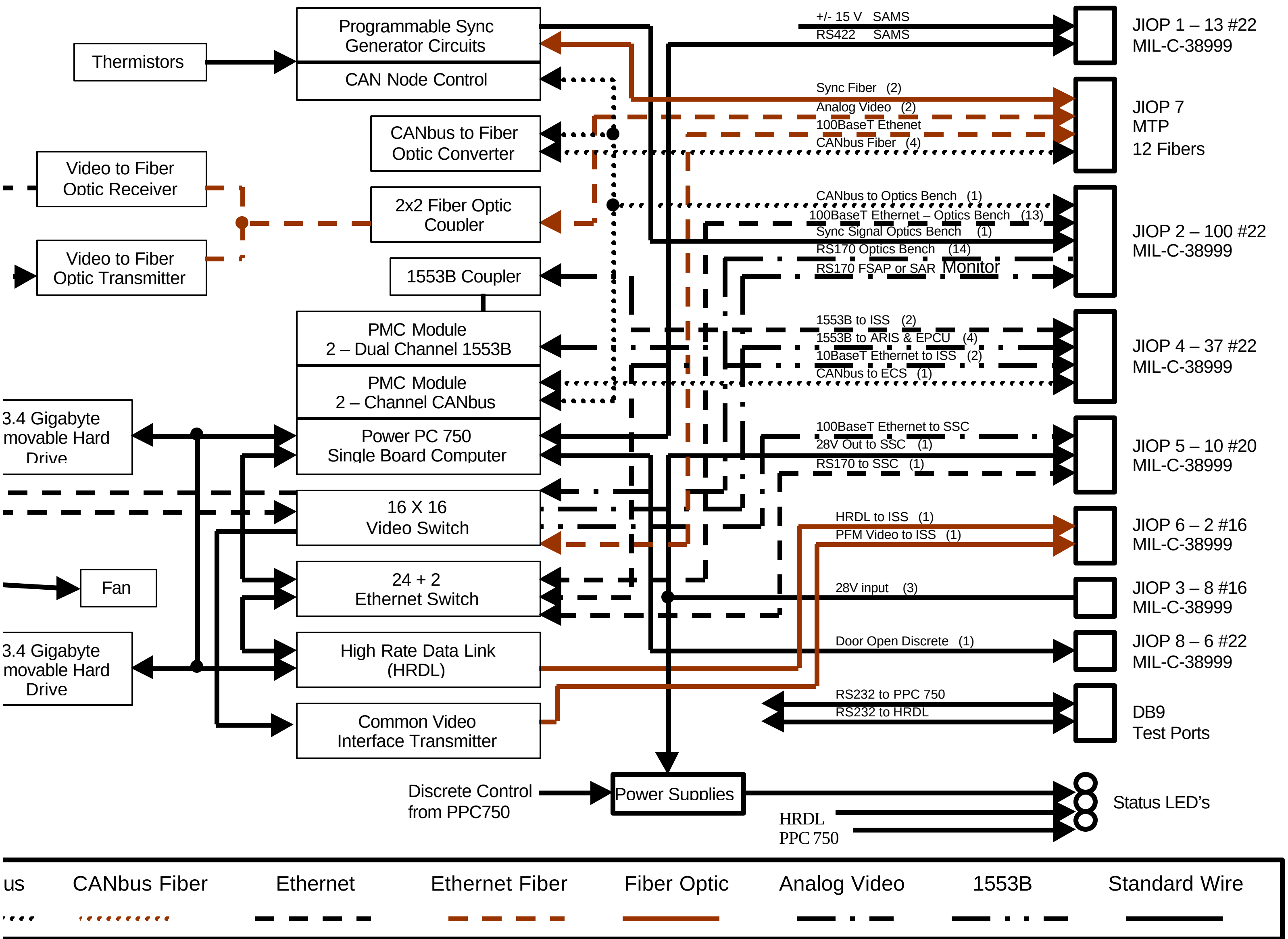
3.2.3 Video Data Display

Video Data to be displayed on a video monitor or the laptop is sent via the 6x6 video switch located in the CIR IOP. Video data to be sent to the ISS monitor must come through the CIR IOP Common Video Interface Transmitter (CVIT) board to be formatted into PFM format prior to sending it to the ISS video system.

3.2.4 Digital Image Buffering

Digital Image Data from the Image Processing Package (IPP) will be buffered on one of two 9 Gigabyte hard disk drives located in the CIR IOP for downlink through the HRDL Interface.

FIGURE 1. FCF IOP – Block Diagram



4.0 FMEA/CIL GROUND RULES AND ASSUMPTIONS

1. The criticality categorization of a failure mode shall be made on the basis of the worst-case potential failure effect regardless of probability of occurrence.

   [Derived from SSP 30234, "Instructions for Preparation of Failure Modes and Effects Analysis and Critical Items List for Space Station", Section 5.14.1]

2. When considering the failure modes for the internal failure of a component/system, all required functional ***inputs*** to the component/system (under analysis) shall be assumed to be present and correct.

   Derived from SSP 30234, Section 5.11]

3. Maintenance procedures or availability of contingency or off-nominal crew (flight or ground) procedures shall not be considered as "unlike" redundancy or as a valid success path in determining the criticality of a component/system failure mode.

   [Derived from SSP 30234, Section 5.14.3]

4. The analysis shall identify ***all potential*** causes for Criticality 1 and 2 failure modes.

   [Derived from SSP 30234, Section 5.5]

5. Identical items which perform the same function(s)/capability(ies), in the same environment, (where the only difference is location) may be analyzed only once, provided that the failure effects for the items are the same.

   [Derived from SSP 30234, Section 5.12]

6. This preliminary FMEA shall be performed to the lowest functional level of analysis necessary to identify critical functions and items.

7. Blockage of orifices shall be considered a credible failure mode.

   [Derived from SSP 30234, Section 5.10.2]

8. The external leakage failure mode of any hardware item from any sources (except mating of two surfaces by inspection capable welding, brazing, or permaswage) shall be considered a credible failure mode.

   [Derived from SSP 30234, Section 5.10.2]

9. Software code and details of human error in an operational scenario shall not be analyzed.

10. Containment vessels, such as combustion chambers and cylinders containing gases, shall be included in the FMEA.

11. Only credible failure modes will be analyzed

5.0 CRITICALITY CATEGORIES

Categories of **1**, **1R**, **1S**, **1SR**, **2**, **2R**, or **3** shall be assigned to all failure modes of the FCF in order to classify all failure mode effects.

[Derived from SSP 30234, section 5.14.1]

1 – A single point failure that could result in loss (failure/damage) of flight hardware, of the ISS itself, or serious injury or loss of flight/ground personnel.

1R – Redundant items/systems, all of which failed, could result in loss (failure/damage) of flight hardware, of the ISS itself, or serious injury or loss of flight/ground personnel.

1S – A single point failure of a system/component designed to provide safety or protection capability against a potentially hazardous condition or event or a single failure point in a safety or hazard monitoring system that causes the system to fail to detect, or operate when needed during the existence of a hazardous condition that could result in loss (failure/damage) of flight hardware, of the ISS itself, or serious injury or loss of flight/ground personnel.

2 – A single point failure that could result in loss or partial loss of a mission critical function.

2R – Redundant items that if failed could result in loss or partial loss of a mission critical function.

3 – All others.

6.0 CRITERIA FOR CRITICAL ITEMS

Upon having completed the listing of failure modes and effects associated with the design, each item/system has been assessed according to a set of rules which are used to determine if am item is ***critical***. The rule or rules by which the assessment is made are referred to as the “Criteria for Critical Items”. Items determined to be ***critical*** are listed separately on a ***critical items list***.

Critical items are items that could result in serious injury, loss of personnel, loss of facilities, or compromise the attainment of mission objectives.

The purpose for a Critical item List (CIL) is to call attention to specific failure modes whose effects are at a high level of severity. Critical Items must be considered and addressed in some manner either by (a) design change, or (b) by compensating provisions within design or operations. *Compensating provisions are*

1. *Design features*
2. *Operational workarounds*
3. *Maintenance actions*
4. *Testing*

5. *0Inspections*

6. *Off-nominal procedures, which are developed to reduce risk or provide a corrective action in response to system level failure effects.*

7. For the FCF, the critical item criterion has been tailored from SSP 30234. The critical items criteria has been simplified and is defined as the following:

An item (hardware device/system with associated failure mode) ***shall be judged to be critical if***:

It is a category 1, or 2 item.

It is a category 1R item that does not meet its failure tolerance requirement.

Criticality 1 and 2 items are single point failure points that could result in worst-case effects that directly impact safety or ability to conduct particular scientific experiments.

7.0 IOP FMEA WORKSHEETS

TABLE I. IOP FMEA Worksheets

Item	Function	Failure Mode & Number	Criticality	Local Effect Worst Case	System Effect	Station/Crew Effects	Potential Causes	Detection Method	Compensating Provision	Time To Detect	Time To Effect
CANbus Connector to Optics Bench	Transfer of input/output for 40 thermistors and 4 RS170A channels in/out of IOP	Connector Failure: Loss of input/output signals. IOP-001	2	Loss of data from 1 or 2 thermistors or switching capability on a RS	Software would flag loss of data from 1 or 2 thermistors or loss of switching capability on an RS170A.	TBD	Loose crimping on one or two connectors wires in I/O connector.	Expect IOP to report loss of input data.	Connector design should be qualified for flight and tested prior to flight. Crimps should be inspected prior to assembly and test.	TBD	TBD
CANbus Connector to Optics Bench	Transfer of input/output on 7 Ethernet channels. 4 interface to IPP, 1 to FCU, and 1 to PI specific Hardware	Loss of Input/Output signals. IOP-002	2	Loss of input/output to FCU	Cannot effectively command and control the FOMA operations	TBD	Wire/pin connections for Ethernet interfacing with FCU become loose and open circuit.	Would expect software flag that IOP cannot read from or send signals to the FCU	Connector design should be qualified for flight and tested prior to flight. Crimps should be inspected prior to assembly and test.	TBD	TBD
Power Connector	Provides power to IOP	Loss of input/output signals IOP-003	2	Significant or complete loss of power	Loss of all IOP functions. Cannot command and control the CIR.	TBD	Wire/pin connections for power connector come loose and open circuit.	Loss of IOP functions.	Power input to IOP and J21 would be checked prior to power up to assure	TBD	TBD
Ethernet connector to the Station Support Computer (SSC)	Provides data interface between IOP and SSC	Connector Failure creates open circuit or loss of power IOP-004	3	Loss of data signal input to SSC from IOP and loss of data signal input to IOP from SSC.	Loss of ability to execute system control functions by crew interface with system.	TBD	Wire/Pin connections for power connector become loose and open circuit.	Loss of SSC data or functionality. Would initiate fault isolation to connector.	System is designed so that command and control interface with IOP can be performed from operations center on ground.	TBD	TBD
Ethernet connector to the Station Support Computer (SSC)	Provides power interface between IOP and SSC	Connector Failure creates loss of power to SSC IOP-005	3	Loss of data signal input to SSC from IOP and loss of data signal input to IOP from SSC. SSC does not function.	Loss of ability to execute system control functions by crew interface with system.	TBD	Wire/Pin connections for power connector become loose and open circuit.	Loss of SSC data or functionality. Would initiate fault isolation to connector.	System is designed so that command and control interface with IOP can be performed from operations center on ground.	TBD	TBD
JIOP1	Connector for SAMS	Connector Failure IOP-006	TBD	Loss of interface to SAMS.	TBD	TBD	Wire/Pin connections for power connector become loose and open circuit.	Expect IOP to report loss of input	Connector design should be qualified for flight and tested prior to flight. Crimps should be inspected prior to assembly and test.	TBD	TBD

Item	Function	Failure Mode & Number	Criticality	Local Effect Worst Case	System Effect	Station/Crew Effects	Potential Causes	Detection Method	Compensating Provision	Time To Detect	Time To Effect
JIOP-2	IOP to Optics Bench Connector	Connector Failure IOP-007	TBD	Loss of interface to Optics Bench	TBD	TBD	Loose Connector, broken wires or pins on connector.	Software should flag loss of IOP interface to Optics Bench.	Connector design should be qualified for flight and tested prior to flight. Crimps should be inspected prior to assembly and test.	TBD	TBD
JIOP-3	EPCU Power Connector	Connector Failure IOP-008	TBD	Loss of power to the IOP	TBD	TBD	Loose Connector, broken wires or pins on connector.	IOP does not power-up	Connector design should be qualified for flight and tested prior to flight. Crimps should be inspected prior to assembly and test.	TBD	TBD
JIOP-4	IOP to Rack Connector	Connector Failure IOP-009	TBD	Loss of interface to ISS, ARIS, EPCU or ECS.	TBD	TBD	Loose Connector, broken wires or pins on connector.	Software should detect loss of interface to ISS, EPCU, ECS, or ARIS	Connector design should be qualified for flight and tested prior to flight. Crimps should be inspected prior to assembly and test.	TBD	TBD
JIOP-5	IOP to SSC Connector	Connector Failure IOP-010	TBD	Loss of power and/or data communications to the SSC	TBD	TBD	Loose Connector, broken wires or pins on connector.	SSC Inoperable. IOP Software should flag for inability to interface to SSC	Connector design should be qualified for flight and tested prior to flight. Crimps should be inspected prior to assembly and test.	TBD	TBD
JIOP-6	HRDL and PFM Video interface to ISS from IOP	Connector Failure IOP-011	TBD	Loss of HRDL connection and/or PFM video interfce to ISS	TBD	TBD	Loose Connector or broken fibers on connector.	IOP software should detect and flag inability to interface to ISS through HRDL or PFM video fiber cables.	Connector design should be qualified for flight and tested prior to flight. Fiber connections should inspected prior to assembly and test.	TBD	TBD
JIOP-7	Rack to Rack Interface	Connector Failure IOP-012	TBD	Loss of one or all Fiber interface connections for Sync, CANbus, Analog Video and 100BaseT Ethernet	TBD	TBD	Loose Connector or broken fibers on connector.	IOP software should detect and flag inability send or receive data thru fiber connections from rack to rack.	Connector design should be qualified for flight and tested prior to flight. Fiber connections should inspected prior to assembly and test.	TBD	
JIOP-8	Door Safety Interlock Switch Connector	Connector Failure IOP-013	TBD	Systems inoperable due to safety interlock system.	TBD	TBD	Loose Connector, broken wires or pins on connector.	Lasers will not energize. IOP Software shoulf flag for safety door interlock activation.	Connector design should be qualified for flight and tested prior to flight. Crimps should be inspected prior to assembly and test.	TBD	TBD
DB-9	Test Ports	Connector Failure IOP-014	TBD	Inability to ground test IOP	TBD	TBD	Loose Connector, broken wires or pins on connector.	Inability to interface to IOP through test port connector during ground test.	Connector design should be qualified for flight and tested prior to flight. Crimps should be inspected prior to assembly and test.	TBD	TBD
TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD

INTENTIONALLY LEFT BLANK

TABLE II. Critical items List

Item Name	Reference to FMEA Worksheets	Failure Modes by Number	Is There Failure detection	Provisions For Design/Test/Operation/Maintenance or Corrective Action
TBD	TBD	TBD	TBD	TBD

APPENDEX A. ACRONYMS AND ABBREVIATIONS

A.1 SCOPE

This appendix lists the acronyms and abbreviations used in this document.

A.2 LIST OF ACRONYMS AND ABBREVIATIONS

CAN	Controller Area Network
CIL	Critical Items List
CIR	Combustion Integrated Rack
CVIT	Common Video Interface Transmitter
FCF	Fluids and Combustion Facility
FIR	Fluids Integrated Rack
FMEA	Failure Modes and Effects Analysis
IOP	Input / Output Processor
IPP	Image Processor Package
IPSU	Image Processing and Storage Unit
ISS	International Space Station
JSC	Johnson Space Center
MM/OD	Micrometeor / Orbital Debris
SAR	Shared Accommodations Rack
SDL	Serial Data Link

APPENDEX B. DEFINITIONS

Failure Mode Number – A number on the FMEA worksheet that identifies a particular hardware item, a specific failure mode, and the corresponding block on the schematic.

Item – A part, component, combination of parts, usually self-contained.

Function – An action or process performed by a sub-system or component by design, which usually involves the transfer of energy and may include the transfer of information. [Note: an alternative definition may apply to passive components of a system such as structure whose “function” is load-bearing capability. Welds, brazings, and epoxy have a function that is to provide adhesion of parts when subjected to forces. “Function” applies to fuels or oxygen in that their function is to transform energy from stored (potential) chemical energy to thermal energy.]

Failure – The inability of a system, subsystem, component or part to perform its required function within specified limits, under specified conditions for a specified duration.

Failure Mode – A description of the manner in which an item can fail.

Criticality – The assigned category of a failure mode based upon the severity of its worst-case effect, which indicates if the failure mode is a single point failure or occurs from the failure of redundant devices.

Local Effect – The consequences a failure mode has on the operation, function, or status of other items (within the payload system), which interface with the specific item being analyzed.

System Effect – The consequence(s) a failure mode has on the operation, function, or status of the overall system.

Hazard – Existing or potential condition that can result in, or contribute to, the injury or loss of personnel or loss of an entire facility.

Single Point Failure – A single item of hardware, the failure of which will lead directly to a hazard, reduce ability to conduct science or result in a mission critical worst case failure effect.